In the Claims:

1. (Original) A device for digital rights management, comprising:

(a) an integrated circuit including:

(i) a processor for:

(A) requesting encrypted digital data, and

(B) decrypting said encrypted digital data, thereby providing decrypted digital data; and

(ii) a player for transforming said decrypted digital data to analog signals; and

(b) a flash memory for storing said encrypted digital data.

2. (Original) The device of claim 1, wherein said encrypted digital data are requested from a server and wherein said requesting of said encrypted digital data includes authenticating said integrated circuit to said server.

3. (Original) The device of claim 1, wherein said integrated circuit is tamper-resistant.

4. (Original) The device of claim 1, wherein said encrypted digital data are audio data.

5. (Original) The device of claim 1, wherein said encrypted digital data are video data.

6. (Original) The device of claim 1, wherein said processor includes an interface for receiving said encrypted digital data.

7. (Original) The device of claim 6, wherein said interface is selected from the group consisting of an ISO7816 interface, a local bus interface, a MMCA interface, a SDA interface, a USB interface and a parallel interface.

8. (Original) The device of claim 1, wherein said integrated circuit has a form factor selected from the group consisting of a SIM form factor, a TQFP form factor, a DIP form factor, a SOP form factor and a BGA form factor.

9. (Canceled)

10. (Original) The device of claim 1, further comprising:

(c) a transceiver for transmitting a request for said encrypted digital data from said processor and for receiving said encrypted digital data.

11. (Original) The device of claim 1, further comprising:

(c) a display mechanism for displaying said analog signals.

12-13. (Canceled)

14. (Original) The device of claim 1, wherein said integrated circuit includes a single said processor.

15. (Original) The device of claim 1, wherein said integrated circuit further includes:

(iii) a ROM for storing management code that is executed by said processor to operate said integrated circuit.

16. (Original) The device of claim 15, wherein said management code is stored only in said ROM.

17. (Original) A system for digital rights management, comprising:

(a) a server for storing encrypted digital data; and

(b) a user platform including:

(i) an integrated circuit that includes:

(A) a processor for:

(I) requesting said encrypted digital data from said server, and

(II) decrypting said encrypted digital data, thereby providing decrypted digital data, and

(B) a player for transforming said decrypted digital data to analog signals, and

(ii) a flash memory for storing said encrypted digital data.

18. (Original) The system of claim 17, wherein said requesting of said encrypted digital data from said server includes authenticating said integrated circuit to said server.

19. (Original) The system of claim 17, wherein said integrated circuit is tamper resistant.

20. (Original) The system of claim 17, wherein said user platform further includes:

(ii) a transceiver for transmitting to said server a request for said encrypted digital data and for receiving said encrypted digital data.

21. (Original) The system of claim 17, wherein said user platform further includes:

(ii) a display mechanism for displaying said analog signals.

22-23. (Canceled)

24. (Original) The system of claim 17, wherein said integrated circuit includes a single said processor.

25. (Original) The system of claim 17, wherein said server is configured to transmit substantially only said encrypted digital data to said user platform.

26. (Original) The system of claim 17, wherein said integrated circuit further includes:

(C) a ROM for storing management code that is executed by said processor to operate said integrated circuit.

27. (Original) The system of claim 26, wherein said management code is stored only in said ROM.

28. (Original) A digital rights management method comprising the steps of:

(a) storing encrypted digital data at a server;

(b) providing an integrated circuit that includes:

(i) a processor operative to:

(A) request said encrypted digital data from the server and

(B) decrypt said encrypted digital data, thereby providing decrypted digital data, and

(ii) a player operative to transform said decrypted digital data to analog signals;

(c) requesting said encrypted digital data from the server, by said processor;

(d) decrypting said encrypted digital data, by said processor, thereby providing said decrypted digital data;

(e) transforming said decrypted digital data to analog signals, by said player; and

(f) storing said encrypted digital data in a flash memory.

29. (Original) The method of claim 28, wherein said requesting includes authenticating said integrated circuit to the server.

30. (Original) The method of claim 29, wherein said authenticating is effected using an asymmetrical algorithm.

31. (Original) The method of claim 30, wherein said asymmetrical algorithm is a RSA algorithm.

32. (Original) The method of claim 30, wherein said asymmetrical algorithm is a ECC algorithm.

33. (Original) The method of claim 28, wherein said decrypting is effected using a symmetrical algorithm.

34. (Original) The method of claim 33, wherein said symmetrical algorithm is a DES algorithm.

35. (Original) The method of claim 33, wherein said symmetrical algorithm is a Rijndael algorithm.

36. (Original) The method of claim 28, wherein said decrypting is effected using at least one key, and wherein the method further comprises the step of:

(g) requesting said at least one key from the server, by said processor.

37. (Original) The method of claim 36, wherein the method further comprises the step of:

(h) storing said at least one key in a nonvolatile memory.

38. (Original) The method of claim 37, further comprising the step of:

(i) encrypting said at least one key, prior to said storing of said at least one key in said nonvolatile memory.

39. (Original) The method of claim 36, further comprising the step of:

(h) configuring the server to send substantially only the encrypted digital data and said at least one key to said integrated circuit.

40. (Canceled)

41. (Original) The method of claim 28, further comprising the step of:

(g) upon detecting an attempt to tamper with said integrated circuit: resetting said integrated circuit.

42. (Original) The method of claim 28, further comprising the step of:

(g) configuring the server to send substantially only the encrypted digital data to said integrated circuit.

43. (Original) The system of claim 17, wherein said digital data are audio data.

44. (Original) The system of claim 17, wherein said digital data are video data.

45. (Original) The method of claim 28, wherein said encrypted digital data are audio data.

46. (Original) The method of claim 28, wherein said encrypted digital data are video data.

47-52. (Canceled)

53. (Original) A digital rights management method, comprising the steps of:

(a) storing encrypted digital data at a server;

(b) providing an integrated circuit that includes:

(i) a processor operative to:

(A) request said encrypted digital data from the server and

(B) decrypt said encrypted digital data, thereby providing decrypted digital data, and

(ii) a player operative to transform said decrypted digital data to analog signals;

(c) requesting said encrypted digital data from the server, by said processor;

(d) receiving said encrypted digital data, by said processor;

(e) storing said received encrypted digital data in a memory separate from said integrated circuit, by said processor;

(f) decrypting said received encrypted digital data, by said processor, thereby providing said decrypted digital data; and

(g) transforming said decrypted digital data to analog signals, by said player.

54. (Original) A digital rights management method, comprising the steps of:

(a) storing encrypted digital data at a server;

(b) providing an integrated circuit that includes:

(i) a processor operative to:

(A) request said encrypted digital data from the server and

(B) decrypt said encrypted digital data, using at least one key, thereby providing decrypted digital data, and

(ii) a player operative to transform said decrypted digital data to analog signals;

(c) requesting said encrypted digital data and said at least one key from the server, by said processor;

(d) storing said at least one key in a nonvolatile memory that is separate from said integrated circuit;

(e) decrypting said encrypted digital data, by said processor, thereby providing said decrypted digital data; and

(f) transforming said decrypted digital data to analog signals, by said player.

55. (New) A digital rights management method comprising the steps of:

(a) storing encrypted digital data at a server;

(b) providing an integrated circuit that includes:

(i) a processor operative to:

(A) request said encrypted digital data from the server and

(B) decrypt said encrypted digital data, thereby providing decrypted digital data, and

(ii) a player operative to transform said decrypted digital data to analog signals;

(c) requesting said encrypted digital data from the server, by said processor;

(d) receiving said encrypted digital data from the server, by said processor;

(e) decrypting said encrypted digital data, by said processor, thereby providing said decrypted digital data; and

(f) transforming said decrypted digital data to analog signals, by said player;

wherein said decrypting and said transforming are effected only after all said encrypted digital data have been received from the server.